

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
Yuusaku OHTA et al. :
Serial No. NEW : **Attn: APPLICATION BRANCH**
Filed August 28, 2003 : **Attorney Docket No. 2003_1214A**
CONTENT DUPLICATION MANAGEMENT :
SYSTEM AND NETWORKED APPARATUS

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEES FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975

Sir:

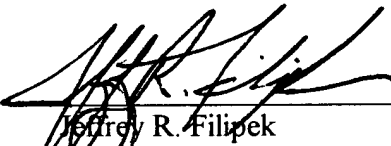
Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-249241, filed August 28, 2002, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Yuusaku OHTA et al.

By



Jeffrey R. Filipek
Registration No. 41,471
Attorney for Applicants

JRF/fs
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
August 28, 2003

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2002年 8月28日

出 願 番 号
Application Number:

特願2002-249241

[ST.10/C]:

[JP 2002-249241]

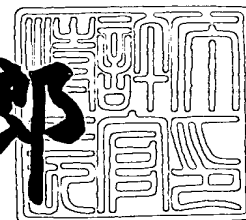
出 願 人
Applicant(s):

松下電器産業株式会社

2003年 6月 5日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3043714

【書類名】 特許願

【整理番号】 2022540327

【提出日】 平成14年 8月28日

【あて先】 特許庁長官 殿

【国際特許分類】 G11B 20/10
G09C 1/00
G06F 12/14

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 太田 雄策

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 山内 弘貴

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 宮▲ざき▼ 雅也

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 松崎 なつめ

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 阿部 敏久

【特許出願人】

 【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社
【代理人】
【識別番号】 100090446
【弁理士】
【氏名又は名称】 中島 司朗
【手数料の表示】
【予納台帳番号】 014823
【納付金額】 21,000円
【提出物件の目録】
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9003742
【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】

情報複製管理ネットワークシステムおよび記録媒体

【特許請求の範囲】

【請求項 1】 複製に関する制限が設けられた情報を複製するための、ネットワークで接続された少なくとも 2 つ以上の端末で構成されるシステムであって、前記第 1 の端末は、前記複製に関する制限が設けられた情報を格納するための記憶手段と、前記複製に関する制限が設けられた情報を前記第 2 の端末に記録するための記録手段と、前記複製に関する制限が設けられた情報のうち、複製の制限に関する部分を更新するための制限情報更新手段と、前記第 2 の端末と通信するための通信手段と、前記第 2 の端末と認証を行うための認証手段とを含み、前記第 1 の端末の前記記憶手段が保有する前記複製に関する制限が設けられた情報を、前記第 2 の端末の前記通信手段による複製要求により、前記第 1 の端末の前記認証手段は、前記第 1 の端末の前記通信手段を介して、前記第 2 の端末の正当性を確認し、さらに前記第 1 の端末が許可した場合に、前記第 1 の端末の前記制限情報更新手段は、前記第 2 の端末に複製する複製の制限に関する情報を更新し、前記第 1 の端末の前記記録手段は前記複製に関する制限が設けられた情報を前記第 2 の端末の記憶手段に複製し、前記第 1 の端末は、自身が保有する複製に関する制限が設けられた情報の複製の制限に関する情報を、前記制限情報更新手段を用いて更新することを特徴とする情報複製管理ネットワークシステム。

【請求項 2】 複製に関する制限が設けられた情報を記録するための記録媒体であって、端末と認証を行うための認証手段と、前記端末の記録手段を用いた複製処理により、複製に関する制限が設けられた情報を格納するための記憶手段とを含み、前記端末からの複製要求により、前記記録媒体の前記認証手段は前記端末の正当性を確認し、前記端末の前記制限情報更新手段は、前記記録媒体に複製する複製の制限に関する情報を更新し、前記端末の前記記録手段は前記複製に関する制限が設けられた情報を記録媒体の記憶手段に複製し、前記端末は、自身が保有する複製に関する制限が設けられた情報の複製の制限に関する情報を前記制限情報更新手段を用いて更新することを特徴とする記録媒体。

【請求項 3】 記録媒体が保有する複製に関する制限が設けられた情報を、端末の複製要求により、前記記録媒体の認証手段は前記端末の正当性を確認し、さらに前記端末が許可した場合に、前記端末の前記制限情報更新手段は、前記記録媒体から複製する複製の制限に関する情報を更新し、前記記録媒体が保有する前記情報の複製に関する制限が設けられた情報を前記記録手段を用いて前記端末の記憶手段に複製し、前記制限情報更新手段を用いて前記記録媒体が保有する複製に関する制限の情報を更新する請求項 1 記載の情報複製管理ネットワークシステム。

【請求項 4】 複製に関する制限として、複製回数が有限な値に制限されている情報を複製するための、請求項 1 または請求項 3 記載の情報複製管理ネットワークシステム。

【請求項 5】 制限情報更新手段として、日付や時刻を管理するための時間管理手段を含む、請求項 1 または請求項 3 記載の情報複製管理ネットワークシステム。

【請求項 6】 複製に関する制限として、決められた日時に複製可能回数が変更されるように設定されている情報を複製するための、請求項 5 記載の情報複製管理ネットワークシステム。

【請求項 7】 複製に関する制限として、情報の複製される時間、および複製された情報を格納する端末が設定されている情報を複製するための、請求項 5 記載の情報複製管理ネットワークシステム。

【請求項 8】 通信手段として、端末が複製しようとする情報を他の全ての端末に問い合わせ、前記複製しようとする情報を保有する端末を特定する手段を含む請求項 1 から請求項 7 のいずれかに記載の情報複製管理ネットワークシステム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、例えば、情報の複製回数を制限して著作権の保護を図る情報管理方法を用いたネットワークシステム、記録媒体に関する。

【 0 0 0 2 】

【従来の技術】

従来、例えばエス・ディー・エム・アイ（SDMI；Secure Digital Music Initiative）における著作権の保護が必要な音楽情報に対しては、該情報の複製に関する管理が行われてきた。具体的には、情報の無制限な複製を防止するために複製の回数を有限にすることや、複製の複製（以下「孫コピー」と呼ぶことがある）の許可・禁止を管理するための複製の世代管理に関する制限などがそれにあたる。

【 0 0 0 3 】

【発明が解決しようとする課題】

ところで、上記のような複製の管理は、主にパーソナルコンピュータ（以下「PC」と呼ぶことがある）や専用レコーダなどの記録装置と、SDカードのような半導体型記録媒体やDVDのような光ディスクなどの記録媒体との間で行われるが、このような複製管理方式の元では、図16に示されるように、例えば、ある記録装置1601から記録媒体1602あるいは1603に複製した複製制限付情報1610を、別の記録装置1604に複製することはできなかった。これは、複製に関する管理情報を、コピー元である記録装置1601が一元管理していることに起因するが、ユーザの利便性という観点からは自由度が低く、必ずしも好ましいものではなかった。

【 0 0 0 4 】

そこで、本発明は上記事情を考慮してなされたもので、ネットワークに接続された少なくとも2つ以上の端末間で、複製に関する制限が設けられた情報を、その制限の範囲内で著作権を保護しつつ自由に複製するための、情報複製管理ネットワークシステムを提供することを目的とする。

また、本発明は、端末から記録媒体に、複製に関する制限が設けられた情報を、その制限の範囲内で著作権を保護しつつ自由に複製するための、記録媒体を提供することを目的とする。

【 0 0 0 5 】

また、本発明は、記録媒体から端末に、複製に関する制限が設けられた情報を

、その制限の範囲内で著作権を保護しつつ自由に複製するための、情報複製管理ネットワークシステムを提供することを目的とする。

また、本発明は、複製に関する制限として時間に関する制限を管理することが可能で、かつその制限の範囲内で著作権を保護しつつ自由に複製するための、情報複製管理ネットワークシステムを提供することを目的とする。

【0006】

また、本発明は、端末間で、複製に関する制限が設けられた情報を、その制限の範囲内で自由な複製を可能にし、かつ端末のうち、どの端末が複製に関する制限が設けられた情報を保有しているかを知ることが可能な情報複製管理ネットワークシステムを提供することを目的とする。

本発明は、情報の複製回数を有限にすることにより、著作権の保護を実現する情報管理に特に有効である。

【0007】

【課題を解決するための手段】

本発明の請求項1記載の発明は、複製に関する制限が設けられた情報を複製するための、ネットワークで接続された少なくとも2つ以上の端末で構成されるシステムであって、前記第1の端末は、前記複製に関する制限が設けられた情報を格納するための記憶手段と、前記複製に関する制限が設けられた情報を前記第2の端末に記録するための記録手段と、前記複製に関する制限が設けられた情報のうち、複製の制限に関する部分を更新するための制限情報更新手段と、前記第2の端末と通信するための通信手段と、前記第2の端末と認証を行うための認証手段とを含み、前記第1の端末の前記記憶手段が保有する前記複製に関する制限が設けられた情報を、前記第2の端末の前記通信手段による複製要求により、前記第1の端末の前記認証手段は、前記第1の端末の前記通信手段を介して、前記第2の端末の正当性を確認し、さらに前記第1の端末が許可した場合に、前記第1の端末の前記制限情報更新手段は、前記第2の端末に複製する複製の制限に関する情報を更新し、前記第1の端末の前記記録手段は前記複製に関する制限が設けられた情報を前記第2の端末の記憶手段に複製し、前記第1の端末は、自身が保有する複製に関する制限が設けられた情報の複製の制限に関する情報を、前記制

限情報更新手段を用いて更新することを特徴とする情報複製管理ネットワークシステムであり、情報を複製する端末と、複製される端末との両方で、複製の制限に関する情報を更新することにより、端末間での自由度の高い複製が行える、という作用を有する。

【 0 0 0 8 】

本発明の請求項 2 記載の発明は、複製に関する制限が設けられた情報を記録するための記録媒体であって、端末と認証を行うための認証手段と、前記端末の記録手段を用いた複製処理により、複製に関する制限が設けられた情報を格納するための記憶手段とを含み、前記端末からの複製要求により、前記記録媒体の前記認証手段は前記端末の正当性を確認し、前記端末の前記制限情報更新手段は、前記記録媒体に複製する複製の制限に関する情報を更新し、前記端末の前記記録手段は前記複製に関する制限が設けられた情報を記録媒体の記憶手段に複製し、前記端末は、自身が保有する複製に関する制限が設けられた情報の複製の制限に関する情報を前記制限情報更新手段を用いて更新することを特徴とする記録媒体であり、情報を複製する端末と、複製される記録媒体との両方で、複製の制限に関する情報を更新することにより、端末と記録媒体間での自由度の高い複製が行える、という作用を有する。

【 0 0 0 9 】

本発明の請求項 3 記載の発明は、請求項 1 記載の情報複製管理ネットワークシステムにおいて、記録媒体が保有する複製に関する制限が設けられた情報を、端末の複製要求により、前記記録媒体の認証手段は前記端末の正当性を確認し、さらに前記端末が許可した場合に、前記端末の前記制限情報更新手段は、前記記録媒体から複製する複製の制限に関する情報を更新し、前記記録媒体が保有する前記情報の複製に関する制限が設けられた情報を前記記録手段を用いて前記端末の記憶手段に複製し、前記制限情報更新手段を用いて前記記録媒体が保有する複製に関する制限の情報を更新することにより、端末と記録媒体間での自由度の高い複製が行える、という作用を有する。

【 0 0 1 0 】

本発明の請求項 4 記載の発明は、請求項 1 または請求項 3 記載の情報複製管理

ネットワークシステムにおいて、複製に関する制限として、複製回数が制限されている情報を、端末間または端末と記録媒体間で複製回数を管理しながら複製を行うことにより、複製回数を有限に保ちながら、かつ自由度の高い複製が行える、という作用を有する。

【 0 0 1 1 】

本発明の請求項 5 記載の発明は、請求項 1 または請求項 3 記載の情報複製管理ネットワークシステムにおいて、制限情報更新手段として、日付や時刻を管理するための時間管理手段を設けることにより、複製に関する制限として時間の概念を管理可能にし、かつ自由度の高い複製が行える、という作用を有する。

本発明の請求項 6 記載の発明は、請求項 5 記載の情報複製管理ネットワークシステムにおいて、複製に関する制限として、決められた日時に複製可能回数が変更されるように設定されている情報を端末間または端末と記録媒体間で複製することにより、複製された情報の時間の概念に伴う複製可能回数の管理を行いながら、かつ自由度の高い複製が行える、という作用を有する。

【 0 0 1 2 】

本発明の請求項 7 記載の発明は、請求項 5 記載の情報複製管理ネットワークシステムにおいて、複製に関する制限として、複製する時間と複製される端末または記録媒体が設定されている情報を端末間または端末と記録媒体間で複製することにより、複製する時間と端末を事前に設定でき、かつ自由度の高い複製が行える、という作用を有する。

【 0 0 1 3 】

本発明の請求項 8 記載の発明は、請求項 1 から請求項 7 記載の情報複製管理ネットワークシステムにおいて、通信手段として、端末が複製しようとする情報を他の全ての端末に問い合わせ、前記複製しようとする情報を保有する端末を特定する手段を設けることにより、複製したい情報を保有する端末または記録媒体を操作する者が事前に知らなくとも複製したい情報を保有する端末または記録媒体を特定することが可能となり、かつ自由度の高い複製が行える、という作用を有する。

【 0 0 1 4 】

【発明の実施の形態】

以下、本発明の実施の形態について、図 1 から図 1 3 を用いて詳細に説明する。

(第 1 の実施の形態)

図 1 に本発明の第 1 の実施の形態に係るネットワークシステムの模式図を示す。図 1 は、端末 0 1 0 1、0 1 0 2、0 1 0 3、0 1 0 4、0 1 0 5 で構成されるネットワークで、通信プロトコルとしては例えばアイピー (IP ; インターネットプロトコル) プロトコルが使用される。図 1 を用いて、まず「メンバ」、「非メンバ」、「グループ」の言葉を定義する。「メンバ」は認証手段をもち、かつ共通秘密情報を有する端末 0 1 0 1、0 1 0 2、0 1 0 3 を指す。「非メンバ」は認証手段を持たない端末 0 1 0 4 や認証手段は持つが共通秘密情報を持たない端末 0 1 0 5 を指す。「グループ」は「メンバ」端末 0 1 0 1、0 1 0 2、0 1 0 3 を要素とする集合の名称である。ここで、共通秘密情報は例えば端末 0 1 0 1 から配布される。このように「メンバ」を要素とする集合「グループ」を定義し、「非メンバ」と区別することにより、複製の範囲を有限なものとして明確に定義することが可能となり、情報の無制限な複製およびグループ外への流出を防止することができる。

【0 0 1 5】

端末を「メンバ」と「非メンバ」に区別した場合、複製について次の 2 種類の組み合わせがあることが分かる。すなわち、「メンバ」から「メンバ」への複製と「メンバ」から「非メンバ」への複製である。ちなみにメンバ、非メンバの概念は相対的なものであるので、非メンバからメンバへの複製はメンバから非メンバへの複製と等価なものとして議論できる。以下に、それぞれの組み合わせの場合の複製手順についてに説明する。説明をより具体的にするため、以下の説明では複製に関する制限として複製回数が N 回に設定されており、その情報にユニークな情報識別番号が割り当てられている情報を元に話を進める。図 2 は前述の複製に関する制限が設けられた情報の概念図である。本来の複製したい情報 0 2 0 1 の先頭にメタデータとして複製制限情報 0 2 0 2 が付加されている。

<メンバ端末からメンバ端末への複製>

図 3 は本発明の第 1 の実施の形態に係る、メンバ端末 0 3 1 0 が保有する複製に関する制限が設けられた情報をメンバ端末 0 3 2 0 に複製するための、それぞれの端末の構成要素を図式化したものである。図 3 において、0 3 1 1、0 3 2 1 はメンバ端末 0 3 1 0 と 0 3 2 0 が互いに情報をやり取りするための通信手段であり、0 3 1 2、0 3 2 2 は互いの端末が同じグループに属するか否かを判断するための認証処理部と、共通秘密情報など認証に必要な情報を格納するための認証手段であり、0 3 1 3、0 3 2 3 は情報を記憶手段に格納し、また、通信手段を介して相手の端末に情報を送信するための記録手段であり、0 3 1 4、0 3 2 4 は複製に関する制限が設けられた情報の制限情報を更新するための制限情報更新手段であり、0 3 1 5、0 3 2 5 は複製に関する制限が設けられた情報を格納するための記憶手段であり、0 3 1 6 は複製に関する制限が設けられた情報である。なお、複製に関する制限が設けられた情報は、秘匿領域に格納され、通常のアクセスはできないこととするのが望ましい。またなお、複製に関する制限が設けられた情報は、その一部あるいは全てが暗号化されていることが望ましい。

【0 0 1 6】

図 1 4 はメンバ端末間での複製に関する制限が設けられた情報を複製する際のフローチャート図である。

以下に図 3 および図 1 4 を用いて、端末 0 3 1 0 が保有する複製に関する制限が設けられた情報をメンバ端末 0 3 2 0 に複製する際の手順を具体的に説明する。

【0 0 1 7】

最初にメンバ端末 0 3 2 0 の利用者は通信手段 0 3 2 1 を用いてメンバ端末 0 3 1 0 に複製要求を送信する（図 1 4 の 1 4 2 1）。なお、この時、利用者は複製回数の制限を上限とする複製個数を同時に指定してもよい。ここでは複製個数は「n」として話を進める。

メンバ端末 0 3 1 0 は自身の通信手段 0 3 1 1 により複製要求を受信すると（図 1 4 の 1 4 1 1）、認証手段 0 3 1 2 は通信手段 0 3 1 1、0 3 2 1 を介し、相手のメンバ端末 0 3 2 0 の認証手段 0 3 2 2 と認証処理を行う（図 1 4 の 1 2

1 2、1 4 2 2)。認証の方法としては、例えばゼロ知識証明を利用したチャレンジアンドレスポンス型のハンドシェイクを利用する。

【0 0 1 8】

認証処理の結果、互いが同じ共通秘密情報を所有していることが分かり、同グループのメンバであることの正当性が確認されると、メンバ端末0 3 1 0は制限情報更新手段0 3 1 4により、要求された複製回数 n と自身の記憶手段0 3 1 5が保有する複製するための情報の可能な複製回数 N との大小を比較し、 n が N より小さいか、または等しいときに次の手順へ進む（図1 4の1 4 1 3）。なお、 n が N より大きい場合は、メンバ端末0 3 1 0の通信手段0 3 1 1はメンバ端末0 3 2 0の複製要求は満足できない旨をメンバ端末0 3 2 0の通信手段0 3 2 1に送信し、この時点で複製不完遂として終了する（図1 4の1 4 1 7）。

【0 0 1 9】

次にメンバ端末0 3 1 0の制限情報更新手段0 3 1 4は、メンバ端末0 3 2 0に複製する情報の複製制限情報を生成する。具体的には、複製回数「 n 」が複製制限情報メタデータとして生成される（図1 4の1 4 1 4）。

生成されたメタデータは記録手段0 3 1 3により複製する情報の先頭に付加される。

【0 0 2 0】

記録手段0 3 1 3は、生成されたメタデータを含む複製するための情報を、通信手段0 3 1 1を介してメンバ端末0 3 2 0の通信手段0 3 2 1に送信する（図1 4の1 4 1 5）。なお、通信時には、前述の認証処理時に一時的な暗号鍵を生成し、その暗号鍵により暗号化された情報を送受することが望ましい。

メンバ端末0 3 2 0の制限情報更新手段0 3 2 4は受信した制限情報に関するメタデータの情報識別番号と、自身の記憶手段0 3 2 5内に保有する情報の全ての情報識別番号とを比較し、同一情報の有無を確認する（図1 4の1 4 2 5）。同一情報がない場合は、受信した複製制限に関するメタデータが記録手段0 3 2 3によりそのまま記憶手段0 3 2 5に記録される（図1 4の1 4 2 7）。同一情報がある場合は、受信した制限情報に関するメタデータの複製回数 n と、自身の記憶手段0 3 2 5が保有する情報の、制限情報に関するメタデータの複製回数 m

との和を新たな複製回数制限情報としてメタデータに上書き更新し、記録手段 0 3 2 3 により、記憶手段に記録する（図 1 4 の 1 4 2 6）。

【 0 0 2 1 】

メンバ端末 0 3 2 0 は複製された情報データを最後まで受信すると、通信手段 0 3 2 1 により受信完了の旨を通知する（図 1 4 の 1 4 2 8）。

メンバ端末 0 3 1 0 はメンバ端末 0 3 2 0 からの受信完了通知を受信すると、制限情報更新手段 0 3 1 4 により、自身の保有する情報の、制限回数に関するメタデータを N から $N - n$ に更新する（図 1 4 の 1 4 1 6）。なお、 $N - n$ が 0 に等しい場合、記録手段 0 3 1 3 は複製制限付情報 0 3 1 6 を記憶手段 0 3 1 5 から消去する。

<メンバ端末から非メンバ端末への複製>

図 4 はメンバ端末 0 4 1 0 が保有する複製に関する制限が設けられた情報を非メンバ端末 0 4 2 0 に複製するための、それぞれの端末の構成要素を図式化したものである。。図 4 において、0 4 1 1、0 4 2 1 はメンバ端末 0 4 1 0 と 0 4 2 0 が互いに情報をやり取りするための通信手段であり、0 4 1 2、0 4 2 2 は互いの端末が同じグループに属するか否かを判断するための認証手段であり、0 4 1 3、0 4 2 3 は情報を記憶手段に格納し、また、通信手段を介して相手の端末に情報を送信するための記録手段であり、0 4 1 4、0 4 2 4 は複製に関する制限が設けられた情報の制限情報を更新するための制限情報更新手段であり、0 4 1 5、0 4 2 5 は複製に関する制限が設けられた情報を格納するための記憶手段であり、0 4 1 6 は複製に関する制限が設けられた情報である。なお、複製に関する制限が設けられた情報は、秘匿領域に格納され、通常のアクセスはできないこととするのが望ましい。またなお、複製に関する制限が設けられた情報は、その一部あるいは全てが暗号化されていることが望ましい。

【 0 0 2 2 】

図 1 5 はメンバ端末から非メンバ端末への、複製に関する制限が設けられた情報を複製する際のフローチャート図である。

以下に図 4 および図 1 5 を用いて、メンバ端末 0 4 1 0 が保有する複製に関する制限が設けられた情報を非メンバ端末 0 4 2 0 に複製する際の手順を具体的に

説明する。

【0023】

最初に非メンバ端末0420の利用者は通信手段0421を用いてメンバ端末0410に複製要求を送信する（図15の1521）。

メンバ端末0410は自身の通信手段0411により複製要求を受信すると（図15の1511）、認証手段0412は通信手段0411、0421を介し、相手のメンバ端末0420の認証手段0422と認証処理を行う（図15の1512、1522）。

【0024】

認証処理の結果、互いが同じ共通秘密情報を所有していないことが分かり、同グループのメンバでないことが確認されると、メンバ端末0410は通信手段0411を用いて複製要求を拒否する旨の通知を送信する（図15の1517、1530）。このようにしてメンバ端末から非メンバ端末への複製を禁止することができる。

【0025】

上述の説明では、メンバ端末0410から非メンバ端末0420への複製を禁止するための手順を述べたが、例えば以下のようにして、図4とまったく同じ構成のメンバ端末0410から非メンバ端末0420への複製を許可する情報があってもよい。

この場合の複製手順を説明するに先だって、複製制限付情報の概念図を図5に示す。複製制限情報0502として、非メンバ端末への複製を認めるフラグが有るとし（図15の1518）、かつ該フラグが「有効」であるとする。

【0026】

この複製制限付情報を元に、以下に該情報の複製手順を説明する。

非メンバ端末0420はメンバ端末0410に通信手段0421を用いて複製要求を送信する（図15の1521）。

メンバ端末0410は通信手段0411により複製要求を受信すると、認証手段0412を用いて、非メンバ端末0420の認証手段0422と認証処理を行う（図15の1511、1522）。

【 0 0 2 7 】

認証処理の結果、複製要求を送信した端末が非メンバー端末であると判別されると、メンバー端末 0 4 1 0 の制限情報更新手段 0 4 1 4 は、複製要求のあった情報 0 4 1 6 の複製制限情報メタデータを読み、複製可能回数が 1 以上であることを確認し（図 1 5 の 1 5 1 3）、非メンバー端末 0 4 2 0 へ送信するメタデータを生成する（図 1 5 の 1 5 1 4）。この生成されたメタデータは複製回数が 0 回であり、非メンバー端末への複製を認めるフラグを「禁止」であるように設定する。

【 0 0 2 8 】

記録手段 0 4 1 3 は上記のように設定されたメタデータを複製される情報の先頭に付加し、通信手段 0 4 1 1 を用いて非メンバー端末 0 4 2 0 に送信する（図 1 5 の 1 5 1 5）。）。なお、通信時には、前述の認証処理時に一時的な暗号鍵を生成し、その暗号鍵により暗号化された情報を送受することが望ましい。

非メンバー端末 0 4 2 0 の記録手段 0 4 2 3 は受信した複製情報を記憶手段 0 4 2 5 に格納する（図 1 5 の 1 5 2 4）。

【 0 0 2 9 】

非メンバー端末 0 4 2 0 は複製情報の受信を完了すると、通信手段 0 4 2 1 を用いてその旨をメンバー端末 0 4 1 0 に送信する（図 1 5 の 1 5 2 8）。

メンバー端末 0 4 1 0 の通信手段 0 4 1 1 が、非メンバー端末 0 4 2 0 からの受信完了通知を受信すると、制限情報更新手段 0 4 1 4 は複製した情報の複製制限情報メタデータに含まれる複製可能回数を「- 1」する（図 1 5 の 1 5 1 6）。なおこの時「- 1」した結果が「0」になる場合は、記録手段 0 4 1 3 は該情報を記憶手段 0 4 1 5 から消去する。

【 0 0 3 0 】

このようにして非メンバー端末 0 4 2 0 へ複製された情報は、複製可能回数が 0 回に設定されているため、以降どのメンバー端末にも複製ができなくなり、また非メンバー端末への複製も禁止されているので、以降どの非メンバー端末へも複製ができなくなる。このようにして元々の複製の総数を増減することなく、非メンバー端末への複製を認めることも可能である。

【 0 0 3 1 】

なお、上述の説明では、非メンバ端末として共通秘密情報を持たない端末を例に用いたが、この他にも認証手段を持たない非メンバ端末や、制限情報更新手段を持たない非メンバ端末があってもよい。この場合のメンバ端末から非メンバ端末への複製についての説明も、上記と同様の手順が適用できる。

以上の説明では、メンバ端末への複製可能回数 N のみが設定されており、非メンバへの複製可能時には N が $N - 1$ になる場合を説明したが、必ずしも上述の実施の形態に限定されるものではなく、例えばメンバ端末への複製回数と、非メンバ端末への複製回数が別々に制限されていてもよい。

【 0 0 3 2 】

上記のように本発明の第 1 の実施の形態では、認証手段を有する端末をネットワークで接続することにより、「メンバ」端末と「非メンバ」端末の区別が可能となり、複製の範囲を有限なものにとどめる事が可能となり、また、複製に関して、複製回数を有限にすることにより著作権を保護しつつ、複製する側とされる側で複製制限情報を管理することで自由度の高い複製が可能となる。

（第 2 の実施の形態）

図 6 に本発明の第 2 の実施の形態に係るネットワークシステムの模式図を示す。図 6 は、端末 0 6 0 1、0 6 0 2、0 6 0 3、0 6 0 4、0 6 0 5 で構成されるネットワークと、記憶媒体 0 6 0 6、0 6 0 7、0 6 0 8、0 6 0 9 からなる。図 6 を用いて、記憶媒体に関する「メンバ」、「非メンバ」、「グループ」の言葉を定義する。記憶媒体に関する「メンバ」とは、認証手段を有し、かつ、メンバ端末や他の記憶媒体と共通の秘密情報を共有する記憶媒体 0 6 0 6、0 6 0 7 のことを指す。また、記憶媒体に関する「非メンバ」とは、認証手段を有しない記憶媒体 0 6 0 8 や、認証手段は有するが共通秘密情報を有しない記憶媒体 0 6 0 9 を指す。記憶媒体に関する「グループ」とはメンバ端末やメンバ記憶媒体を要素とする集合の名称を指す。このように「メンバ」、「非メンバ」、「グループ」の言葉の定義を記憶媒体に対して拡張することにより、端末への複製に限定されることなく、記憶媒体への複製を含めて、複製の範囲を有限なものとして明確に定義することが可能となり、情報の無制限な複製およびグループ外への流出を防止することができる。

【 0 0 3 3 】

図 7 は、端末 0 7 1 0 が保有する複製制限付きの情報 0 7 1 6 を記憶媒体 0 7 0 1 に複製するための構成要素および接続関係を図示した模式図である。図 7 において、記憶媒体 0 7 0 1 は端末 0 7 1 0 と認証処理を行うための認証手段 0 7 0 2 と、複製制限付き情報を格納するための記憶手段 0 7 0 3 から構成される。なお、複製に関する制限が設けられた情報は、秘匿領域に格納され、通常のアクセスはできないこととするのが望ましい。またなお、複製に関する制限が設けられた情報は、その一部あるいは全てが暗号化されていることが望ましい。

【 0 0 3 4 】

以下に図 7 を用いて、端末 0 7 1 0 が保有する複製に関する制限が設けられた情報を記憶媒体 0 7 0 1 に複製する際の手順を具体的に説明する。複製する複製制限付情報としては前述の図 2 を使用する。

最初に端末 0 7 1 0 の利用者は、端末 0 7 1 0 の記憶手段 0 7 1 5 が保有する複製制限付情報 0 7 1 6 を複製するための操作を行う。なお、この時利用者は複製回数の制限を上限とする複製個数を同時に指定してもよい。ここでは複製個数は「 n 」として話を進める。

【 0 0 3 5 】

端末 0 7 1 0 は、利用者からの複製操作を認識すると、認証手段 0 7 1 2 を用いて記憶媒体 0 7 0 1 の認証手段 0 7 0 2 と認証処理を開始する。

認証処理の結果、互いが同グループのメンバーであることが確認されると、次に端末 0 7 1 0 は制限情報更新手段 0 7 1 4 により、要求された複製個数 n と自身の記憶手段 0 7 1 5 が保有する複製するための情報の可能な複製回数 N との大きさを比較し、 n が N より小さいか、または等しいときに次の手順へ進む。なお、 n が N より大きい場合は、端末 0 7 1 0 はこの時点で複製不完遂として処理を終了する。またなお、認証処理の結果、互いが同グループのメンバーでないことが確認された場合の処理手順については後述する。

【 0 0 3 6 】

次に端末 0 7 1 0 の制限情報更新手段 0 7 1 4 は、記録媒体 0 7 0 1 の記憶手段 0 7 0 3 内の複製制限に関する情報を確認し、複製しようとしている情報と同

じ情報識別番号を持つ情報の存在を確認する。確認の結果、同じ情報識別番号を持つ情報が存在した場合、その情報の複製可能回数を m として、記録媒体 0 7 0 1 が保有する該情報の複製可能回数を $n + m$ に設定し、また端末 0 7 1 0 が保有する該情報の複製可能回数を $N - n$ に設定し、複製処理を終了する。なお、 $N - n$ が 0 に等しい場合、記録手段 0 7 1 3 は複製制限付情報 0 7 1 6 を記憶手段 0 7 1 5 から消去する。

【 0 0 3 7 】

あるいは、制限情報更新手段 0 7 1 4 による同一識別情報を持つ情報の存在の確認の結果、記録媒体 0 7 0 1 が同一情報を保有していないことが確認されると、記録媒体 0 7 0 1 に複製可能回数が n である複製制限情報を生成する。

生成された複製制限情報は記録手段 0 7 1 3 により複製する情報の先頭に付加される。

【 0 0 3 8 】

記録手段 0 7 1 3 は、生成されたメタデータを含む複製するための情報を、記録媒体 0 7 0 1 の記憶手段 0 7 0 3 に記録する。

端末 0 7 1 0 は複製した情報を、記録媒体 0 7 0 1 の記憶手段 0 7 0 3 に最後まで記録すると記録処理を終了する。

最後に、メンバ端末 0 7 1 0 は制限情報更新手段 0 7 1 4 により、自身の保有する情報の、制限回数に関するメタデータを N から $N - n$ に更新する。なお、 $N - n$ が 0 に等しい場合、記録手段 0 7 1 3 は複製制限付情報 0 7 1 6 を記憶手段 0 7 1 5 から消去する。

【 0 0 3 9 】

なお、上述の説明では複製制限付情報を保有する端末 0 7 1 0 と記録媒体 0 7 0 1 を直接接続した場合の複製手順について説明したが、この他にも例えば図 8 のように記録媒体 0 8 0 1 が接続された端末 0 8 2 0 とは別の端末 0 8 1 0 が保有する複製制限付情報 0 8 1 6 を複製することも可能である。この場合、記録媒体 0 8 0 1 の認証手段 0 8 0 2 は、端末 0 8 2 0 の通信手段 0 8 2 1 に直接接続される。その他の構成要素については前述のとおりである。この場合の複製手順を以下に説明する。

【 0 0 4 0 】

まず端末 0 8 1 0 は通信手段 0 8 1 1 を用いて端末 0 8 2 0 に複製制限付情報 0 8 1 6 を複製する旨を通知する。

次に端末 0 8 2 0 の通信手段 0 8 2 1 が複製する旨を受信すると、記録媒体 0 8 0 1 の認証手段 0 8 0 2 と端末 0 8 1 0 の認証手段 0 8 1 2 の間で通信手段 0 8 1 1 および 0 8 2 1 を介して認証処理を開始する。

【 0 0 4 1 】

認証処理の結果、互いが同グループのメンバーであることが確認されると、次に端末 0 8 1 0 は制限情報更新手段 0 8 1 4 により、複製個数 n と自身の記憶手段 0 8 1 5 が保有する複製するための情報の可能な複製回数 N との大小を比較し、 n が N より小さいか、または等しいときに次の手順へ進む。なお、 n が N より大きい場合は、端末 0 8 1 0 はこの時点で複製不完遂として処理を終了する。またなお、認証処理の結果、互いが同グループのメンバーでないことが確認された場合の処理手順については後述する。

【 0 0 4 2 】

次に、端末 0 8 1 0 の制限情報更新手段 0 8 1 4 は、複製する情報に付加する複製制限情報を生成する。具体的には複製可能回数 n を設定する。

複製制限情報を生成後、端末 0 8 1 0 の記録手段 0 8 1 3 は通信手段を介し、複製制限付情報 0 8 1 6 を端末 0 8 2 0 に送信する。)。なお、通信時には、前述の認証処理時に一時的な暗号鍵を生成し、その暗号鍵により暗号化された情報を送受することが望ましい。

【 0 0 4 3 】

端末 0 8 2 0 が複製された複製制限付情報 0 8 1 6 を受信すると、制限情報更新手段 0 8 2 4 は、記録媒体 0 8 0 1 の記憶手段 0 8 0 3 内に同一の情報識別番号をもつ情報の存在を確認する。確認の結果、同じ情報識別番号を持つ情報が存在した場合、その情報の複製可能回数を m として、受信した複製制限情報の複製可能回数を $n + m$ に設定し、記録手段 0 8 2 3 により記録媒体 0 8 0 1 の記憶手段 0 8 0 3 に記録する。あるいは、同一識別情報を持つ情報を記録媒体 0 8 0 1 が保有していないことが確認されると、記録手段 0 8 2 3 は受信した複製制限情

報をそのまま記録する。

【 0 0 4 4 】

端末 0 8 2 0 は複製された情報データを最後まで受信すると、通信手段 0 8 2 1 により受信完了の旨を通知する。

メンバ端末 0 8 1 0 はメンバ端末 0 8 2 0 からの受信完了通知を受信すると、制限情報更新手段 0 8 1 4 により、自身の保有する情報の、制限回数に関するメタデータを N から $N - n$ に更新する。なお、 $N - n$ が 0 に等しい場合、記録手段 0 8 1 3 は複製制限付情報 0 8 1 6 を記憶手段 0 8 1 5 から消去する。

【 0 0 4 5 】

以上の説明では、認証処理の結果、同一グループのメンバであると確認された場合の複製手順について述べたが、同一グループのメンバでないと確認された場合の処理手順については第 1 の実施の形態で述べた処理手順と同様である。

上記のように本発明の第 2 の実施の形態では、記録媒体を「メンバ」と「非メンバ」に区別することにより、本発明の第 1 の実施の形態で述べた効果に加え、複製する端末と複製される記録媒体で複製制限情報を管理することで、自由度の高い複製が可能となる。

(第 3 の実施の形態)

図 9 は本発明の第 3 の実施の形態に係る端末 0 9 1 0 と記録媒体 0 9 0 1 の各構成要素および接続関係を図示した模式図である。各構成要素については、複製制限付情報 0 9 1 6 が記録媒体 0 9 0 1 の記憶手段 0 9 0 3 に格納されている以外は、図 7 と同様であるので説明を割愛する。

【 0 0 4 6 】

以下に図 9 を用いて、記憶媒体 0 9 0 1 が保有する複製に関する制限が設けられた情報を、端末 0 9 1 0 に複製する際の手順を具体的に説明する。複製する複製制限付情報としては前述の図 2 を使用する。なお、複製に関する制限が設けられた情報は、秘匿領域に格納され、通常のアクセスはできないこととするのが望ましい。またなお、複製に関する制限が設けられた情報は、その一部あるいは全てが暗号化されていることが望ましい。

【 0 0 4 7 】

最初に端末 0 9 1 0 の利用者は記録媒体 0 9 0 1 の記憶手段 0 9 1 5 が保有する複製制限付情報 0 9 1 6 を複製するための操作を行う。なお、この時利用者は複製回数の制限を上限とする複製個数を同時に指定してもよい。ここでは複製個数は「 n 」として話を進める。

端末 0 9 1 0 は、利用者からの複製操作を認識すると、認証手段 0 9 1 2 を用いて記憶媒体 0 9 0 1 の認証手段 0 9 0 2 と認証処理を開始する。

【 0 0 4 8 】

認証処理の結果、互いが同グループのメンバーであることが確認されると、次に端末 0 9 1 0 は制限情報更新手段 0 9 1 4 により、要求された複製個数 n と記録媒体 0 9 0 1 の記憶手段 0 9 0 3 が保有する複製するための情報の可能な複製回数 N との大小を比較し、 n が N より小さいか、または等しいときに次の手順へ進む。なお、 n が N より大きい場合は、端末 0 9 1 0 はこの時点で複製不完遂として処理を終了する。またなお、認証処理の結果、互いが同グループのメンバーでないことが確認された場合の処理手順については後述する。

【 0 0 4 9 】

次に端末 0 9 1 0 の制限情報更新手段 0 9 1 4 は、自身の記憶手段 0 9 1 5 内の複製制限に関する情報を確認し、複製しようとしている情報と同じ情報識別番号を持つ情報の存在を確認する。確認の結果、同じ情報識別番号を持つ情報が存在した場合、その情報の複製可能回数を m として、記録媒体 0 9 0 1 が保有する該情報の複製可能回数を $N - n$ に設定し、また端末 0 9 1 0 が保有する該情報の複製可能回数を $n + m$ に設定し、複製処理を終了する。なお、 $N - n$ が 0 に等しい場合、記録手段 0 9 1 3 は、複製制限付情報 0 9 1 6 を記録媒体 0 9 0 1 の記憶手段 0 9 0 3 から消去する。

【 0 0 5 0 】

あるいは、制限情報更新手段 0 9 1 4 による同一識別情報を持つ情報の存在の確認の結果、記憶手段 0 9 1 5 が同一情報を保有していないことが確認されると、複製可能回数が n である複製制限情報を生成する。

生成された複製制限情報は記録手段 0 9 1 3 により複製する情報の先頭に付加される。

【 0 0 5 1 】

記録手段 0 9 1 3 は、生成されたメタデータを含む複製するための情報を、端末 0 9 1 0 の記憶手段 0 9 1 5 に記録する。

端末 0 9 1 0 は複製した情報を、自身の記憶手段 0 9 1 5 に最後まで記録すると記録処理を終了する。

最後に、メンバ端末 0 9 1 0 は制限情報更新手段 0 9 1 4 により、記録媒体 0 9 0 1 の保有する情報の、制限回数に関するメタデータを N から $N - n$ に更新する。なお、 $N - n$ が 0 に等しい場合、記録手段 0 9 1 3 は複製制限付情報 0 9 1 6 を記憶手段 0 9 0 3 から消去する。

【 0 0 5 2 】

なお、上述の説明では複製制限付情報を保有する端末 0 9 1 0 と記録媒体 0 9 0 1 を直接接続した場合の複製手順について説明したが、この他にも例えば図 1 0 のように記録媒体 1 0 0 1 が接続された端末 1 0 2 0 とは別の端末 1 0 1 0 に複製制限付情報 1 0 1 6 を複製することも可能である。この場合、記録媒体 1 0 0 1 の認証手段 1 0 0 2 は、端末 1 0 2 0 の通信手段 1 0 2 1 に直接接続される。その他の構成要素については前述のとおりである。この場合の複製手順を以下に説明する。

【 0 0 5 3 】

まず端末 1 0 1 0 は通信手段 1 0 1 1 を用いて端末 1 0 2 0 に複製制限付情報 1 0 1 6 の複製要求を送信する。

端末 1 0 2 0 の通信手段 1 0 2 1 は、複製要求を受信すると、記録媒体 1 0 0 1 の認証手段 1 0 0 2 と端末 1 0 1 0 の認証手段 1 0 1 2 の間で通信手段 1 0 1 1 および 1 0 2 1 を介して認証処理を開始する。

【 0 0 5 4 】

認証処理の結果、互いが同グループのメンバであることが確認されると、次に端末 1 0 2 0 は制限情報更新手段 1 0 2 4 により、複製個数 n と記憶媒体 1 0 0 1 の記憶手段 1 0 0 3 が保有する複製するための情報の可能な複製回数 N との大小を比較し、 n が N より小さいか、または等しいときに次の手順へ進む。なお、 n が N より大きい場合は、端末 1 0 2 0 はこの時点で複製不完遂として処理を終

了する。またなお、認証処理の結果、互いが同グループのメンバでないことが確認された場合の処理手順については後述する。

【 0 0 5 5 】

次に、端末 1 0 2 0 の制限情報更新手段 1 0 2 4 は、複製する情報に付加する複製制限情報を生成する。具体的には複製可能回数 n を設定する。

複製制限情報を生成後、端末 1 0 2 0 の記録手段 1 0 2 3 は通信手段を介し、複製制限付情報 1 0 1 6 を端末 1 0 2 0 に送信する。)。なお、通信時には、前述の認証処理時に一時的な暗号鍵を生成し、その暗号鍵により暗号化された情報を送受することが望ましい。

【 0 0 5 6 】

端末 1 0 1 0 が複製された複製制限付情報 1 0 1 6 を受信すると、制限情報更新手段 1 0 1 4 は、自身の記憶手段 1 0 1 5 内に同一の情報識別番号をもつ情報の存在を確認する。確認の結果、同じ情報識別番号を持つ情報が存在した場合、その情報の複製可能回数を m として、受信した複製制限情報の複製可能回数を $n + m$ に設定し、記録手段 1 0 1 3 により記憶手段 1 0 1 5 に記録する。あるいは、同一識別情報を持つ情報を記憶手段 1 0 1 5 が保有していないことが確認されると、記録手段 1 0 1 3 は受信した複製制限情報をそのまま記録する。

【 0 0 5 7 】

端末 1 0 1 0 は複製された情報データを最後まで受信すると、通信手段 1 0 1 1 により受信完了の旨を通知する。

端末 1 0 2 0 は端末 1 0 1 0 からの受信完了通知を受信すると、制限情報更新手段 1 0 2 4 により、記録媒体 1 0 0 1 の保有する情報の、制限回数に関するメタデータを N から $N - n$ に更新する。なお、 $N - n$ が 0 に等しい場合、記録手段 1 0 2 3 は複製制限付情報 1 0 1 6 を記憶手段 1 0 0 3 から消去する。

【 0 0 5 8 】

以上の説明では、認証処理の結果、同一グループのメンバであると確認された場合の複製手順について述べたが、同一グループのメンバでないと確認された場合の処理手順については第 1 の実施の形態で述べた処理手順と同様である。

上記のように本発明の第 3 の実施の形態では、本発明の第 1 の実施の形態で述

べた効果に加え、複製する記録媒体とされる端末で複製制限情報を管理することで自由度の高い複製が可能となる。

（第４の実施の形態）

図１１は、本発明の第４の実施の形態に係る、制限情報更新手段１１０１と記憶手段１１１０、記録手段１１２０の各構成要素および接続関係を図示した模式図である。記憶手段１１１０は、複製制限情報１１１２として、設定時間１１１３、現在の複製可能回数１１１４、設定時間後の複製可能回数１１１５が設定されている複製制限付情報１１１１を保有している。また制限情報更新手段１１０１は日付や時刻などの時間を管理するための時間管理手段１１０２を含んでおり、この機能により、該時間管理手段１１０２は記憶手段１１１０内の有効期限情報１１１３を管理することができるようになっている。なお、図１１における記憶手段１１１０は端末の構成要素であっても良いし、記録媒体の構成要素であっても良い。またなお、複製に関する制限が設けられた情報は、秘匿領域に格納され、通常のアクセスはできないこととするのが望ましい。また、複製に関する制限が設けられた情報は、その一部あるいは全てが暗号化されていることが望ましい。

【００５９】

以下に図１１を用いて、設定時間情報１１１３を管理する際の手順を具体的に説明する。

時間管理手段１１０２は、設定時間１１１３と同じ時間を自身で管理し、設定された時刻になると、制限情報更新手段１１０１は現在の複製可能回数１１１４の値を、設定時間後の複製可能回数の値１１１５に更新する。なお、設定時間後の複製可能回数が０の時は、記録手段１１２０により、その複製制限付情報を消去する。またなお、ある特定のグループ内で、ある特定の複製制限付情報を保有する各メンバ端末および各メンバ記録媒体が管理する現在の複製可能回数の総和は、設定時間後の複製可能回数の総和に等しいことは言うまでもない。また、記録媒体の記憶手段は、設定時間時に必ずしも端末の制限情報更新手段と接続されているわけではないが、記録媒体の時間管理に関しては、端末に接続された時点で時間管理手段が設定時間を確認し、設定時間を超えていた場合には即座に現在

の複製可能回数を設定時間後の複製可能回数に更新することにより同様の効果が得られる。

【 0 0 6 0 】

上記のように本発明の第 4 の実施の形態では、制限情報更新手段 1 1 0 1 に時間管理手段 1 1 0 2 を設けることにより、本発明の第 1 の実施の形態または第 3 の実施の形態で述べた効果に加え、時間に基づいた複製可能回数の更新が可能となる。

（第 5 の実施の形態）

図 1 2 は、本発明の第 5 の実施の形態に係る、制限情報更新手段 1 2 0 1 と記憶手段 1 2 1 0、記録手段 1 2 2 0、通信手段 1 2 3 0 の各構成要素および接続関係を図示した模式図である。記憶手段 1 2 1 0 は、複製制限情報 1 2 1 2 として、複製時間 1 2 1 3、IP アドレスやあるいはメンバにユニークな識別番号により指定される複製先のメンバ 1 2 1 4、複製する際の複製個数 1 2 1 5 が設定されている複製制限付情報 1 2 1 1 を保有している。また制限情報更新手段 1 2 0 1 は日付や時刻などの時間を管理するための時間管理手段 1 2 0 2 を含んでおり、この機能により、該時間管理手段 1 2 0 2 は記憶手段 1 2 1 0 内の有効期限情報 1 2 1 3 を管理することができるようになっている。なお、図 1 2 における記憶手段 1 2 1 0 は端末の構成要素であっても良いし、記録媒体の構成要素であっても良い。またなお、複製に関する制限が設けられた情報は、秘匿領域に格納され、通常のアクセスはできないこととするのが望ましい。また、複製に関する制限が設けられた情報は、その一部あるいは全てが暗号化されていることが望ましい。

【 0 0 6 1 】

以下に図 1 2 を用いて、複製時間 1 2 1 3 を管理する際の手順を具体的に説明する。

時間管理手段 1 2 0 2 は、複製時間 1 2 1 3 と同じ時間を自身で管理し、設定された時刻になると、記録手段 1 2 2 0 は、通信手段 1 2 3 0 を介して、複製先メンバ 1 2 1 4 に指定されるメンバとの間で認証処理を開始する。以降の処理手順については、第 1 の実施の形態から第 3 の実施の形態で述べた方法と同様であ

るので説明を省略する。

【 0 0 6 2 】

上記のように本発明の第 5 の実施の形態では、制限情報更新手段 1 2 0 1 に時間管理手段 1 2 0 2 を設けることにより、本発明の第 1 の実施の形態または第 3 の実施の形態で述べた効果に加え、時間に基づいた複製処理の開始が可能となる。

(第 6 の実施の形態)

図 1 3 は、本発明の第 6 の実施の形態に係る、ある特定の複製制限付情報を検索し、複製したい端末 1 3 0 1 と、検索対照の情報を保有する端末 1 3 0 2、接続された記録媒体が検索対象情報を保有する端末 1 3 0 3、検索対象の情報を保有しない端末 1 3 0 4 間での該情報検索時の模式図である。

【 0 0 6 3 】

以下に図 1 3 を用いて、複製したい情報を検索するときの手順を具体的に説明する。

まず情報を検索したい端末 1 3 0 1 は、自身と同一グループに属するメンバ端末 1 3 0 2、1 3 0 3、1 3 0 4 へ、同報通信的な方法を用いて、検索したい情報の情報識別番号を送信する(図 1 3 の矢印 1 3 1 1、1 3 1 2、1 3 1 3)。

【 0 0 6 4 】

各端末の制限情報更新手段は、自身の記憶手段および、自身に接続された記録媒体の記憶手段が保有する複製制限付情報の情報識別番号を管理しており、受信した検索中の情報の情報識別番号と、自身が管理する情報識別番号とを比較し、同一の情報がある場合には、送信元の端末 1 3 0 1 に該情報を保有している旨を返信する(図 1 3 の矢印 1 3 2 1、1 3 2 2)。)。なお、通信方法としては、例えば共通秘密情報を利用した暗号通信を利用することが望ましい。

【 0 0 6 5 】

この方法により、複製したい情報を管理する端末を特定することができ、複製手順を開始することが可能となる。以降の処理手順については、第 1 の実施の形態から第 3 の実施の形態で述べた方法と同様であるので説明を省略する。

なお、検索中の情報を管理する端末 2 台以上あった場合には、例えば最初に保

有する旨を返信してきた端末から複製することにする。あるいは、検索中の情報を管理する端末は、保有する旨のみを返信するのではなく、保有する複製可能回数も同時に返信するとし、より多くの複製可能回数を有する端末から複製するとしても良い。また他にも、より近い端末から複製する方法や、より通信帯域の広い端末から複製するなどとしても良い。またなお、ある端末からの複製要求があり、要求された複製個数が、自身の保有する複製可能個数より多かった場合に、上記通信方法を用いて、他に同一情報を保有する端末を特定し、要求された複製個数分を、複数台の端末から合わせて複製することにより、該複製要求情報を満足する方法もある。

【 0 0 6 6 】

上記のように本発明の第 6 の実施の形態では、通信手段として、複製したい情報を同報通信的に問い合わせ、複製したい情報を保有する端末を特定する手段を設けることにより、本発明の第 1 の実施の形態から第 5 の実施の形態で述べた効果に加え、複製制限付情報を保有する端末を特定することが可能となる。

（その他の変形例）

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

【 0 0 6 7 】

（1）上記の各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記 RAM 又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。

【 0 0 6 8 】

（2）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD（Blu-ray Disc）、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0069】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0070】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(3) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0071】

【発明の効果】

以上のように、本発明によれば、ネットワークで接続された端末間で、複製に関する制限が設けられた情報を複製する際、複製する側とされる側の両方の複製の制限に関する情報を更新することにより、複製する側が複製に関する情報を一元管理していた従来技術と比べ、より自由度の高い複製が可能になる、という効果が得られる。

【0072】

また、請求項2に係る発明によれば、端末から記録媒体に、複製に関する制限

が設けられた情報を複製する際、複製する側とされる側の両方の複製の制限に関する情報を更新することにより、複製する側が複製に関する情報を一元管理していた従来技術と比べ、より自由度の高い複製が可能になる、という効果が得られる。

【0073】

また、請求項3に係る発明によれば、記録媒体から端末に、複製に関する制限が設けられた情報を複製する際、複製する側とされる側の両方の複製の制限に関する情報を更新することにより、記録媒体に複製した端末にしか複製できなかったしていた従来技術と比べ、より自由度の高い複製が可能になる、という効果が得られる。

【0074】

また、請求項5に係る発明によれば、制限情報更新手段として、時間を管理する手段を設けることにより、複製に関する制限として、時間の概念を用いることが可能となり、より多岐に渡る複製制限を設けることが可能になる、という効果が得られる。

また、請求項8に係る発明によれば、通信手段として、端末が複製しようとする情報を他の全ての端末に問い合わせ、複製しようとする情報を保有する端末を特定する手段を設けることにより、複製する情報を保有する端末または記録媒体を必ずしも利用者や各端末が管理する必要は無く、管理負荷の低減という効果が得られる。

【図面の簡単な説明】

【図1】

ネットワーク端末における「メンバ」、「非メンバ」、「グループ」の概念図

【図2】

複製回数制限付情報の概念図

【図3】

メンバ端末間の複製制限付情報複製の構成図

【図4】

メンバ端末・非メンバ間の複製制限付情報複製の構成図

【図 5】

非メンバ端末への複製許可フラグを含む複製回数制限付情報の概念図

【図 6】

端末・記録媒体に関する「メンバ」、「非メンバ」、「グループ」の概念図

【図 7】

端末が保有する複製制限付情報を直接接続された記録媒体へ複製する際の構成図

【図 8】

端末が保有する複製制限付情報を別の端末に接続された記録媒体へ複製する際の構成図

【図 9】

記録媒体が保有する複製制限付情報を直接接続された端末へ複製する際の構成図

【図 1 0】

端末に接続された記録媒体が保有する複製制限付情報を、別の端末へ複製する際の構成図

【図 1 1】

設定時間後に複製可能回数が更新される情報を管理するための構成図

【図 1 2】

設定時間後に複製処理が実行される情報を管理するための構成図

【図 1 3】

複製したい情報を検索する際の端末間の通信に関する模式図

【図 1 4】

メンバ端末間での複製手順に関するフローチャート

【図 1 5】

メンバ端末から非メンバ端末への複製手順に関するフローチャート

【図 1 6】

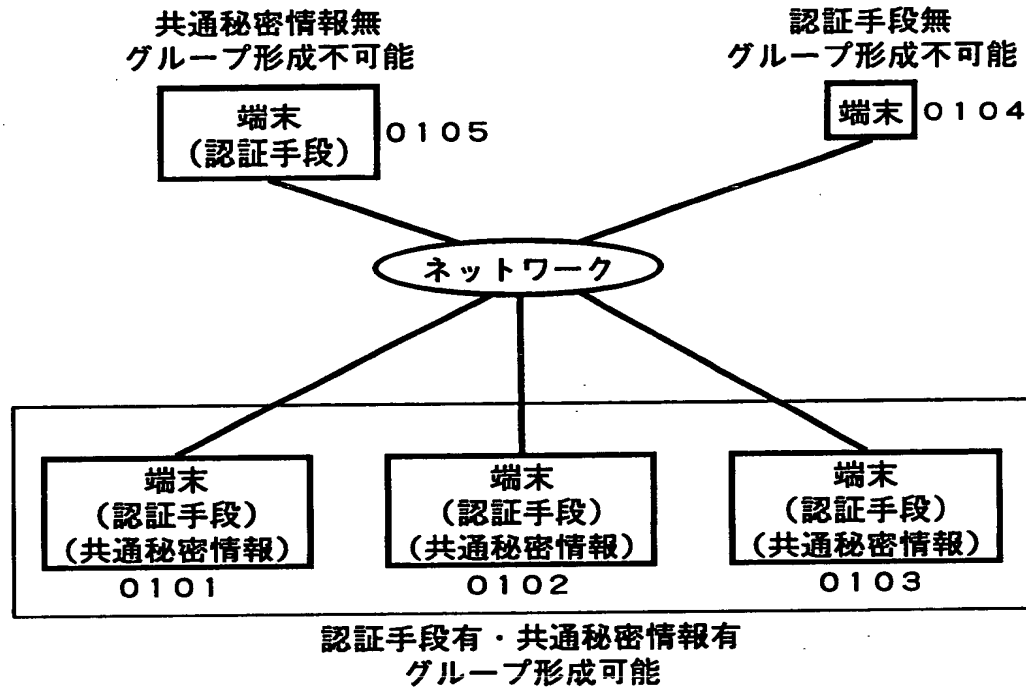
従来の複製制限付情報の複製方法の概念図

【符号の説明】

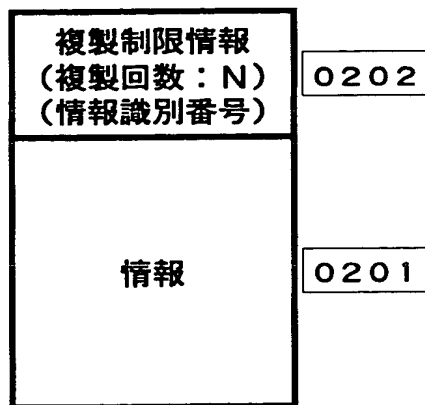
- 0 3 1 0 メンバ端末
- 0 3 1 1 通信手段
- 0 3 1 2 認証手段
- 0 3 1 3 記録手段
- 0 3 1 4 制限情報更新手段
- 0 3 1 5 記憶手段
- 0 3 1 6 制限情報付き情報

【書類名】 図面

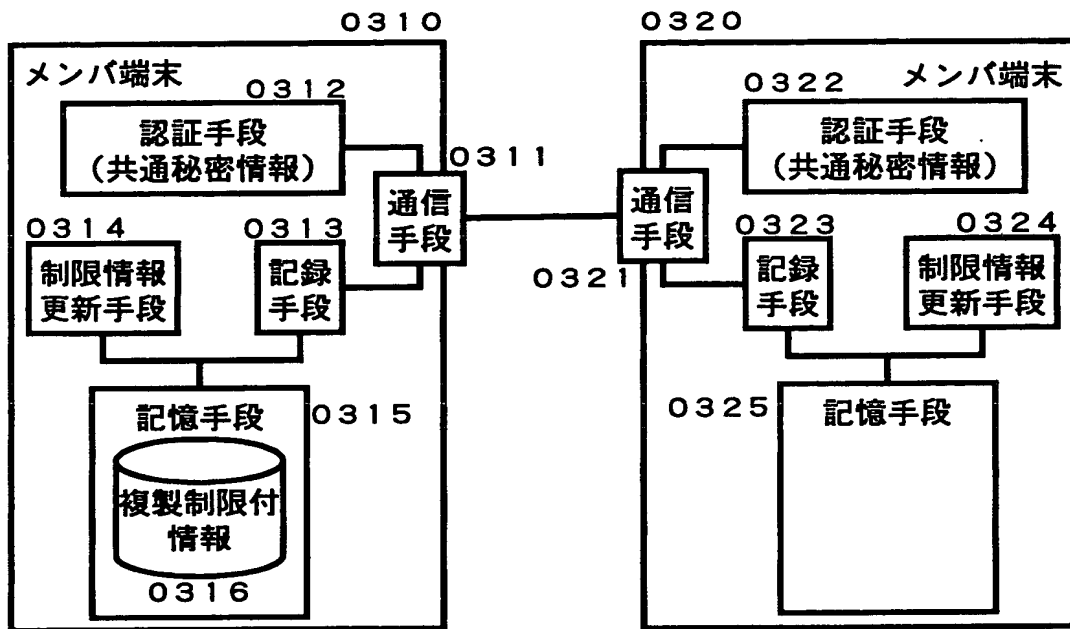
【図 1】



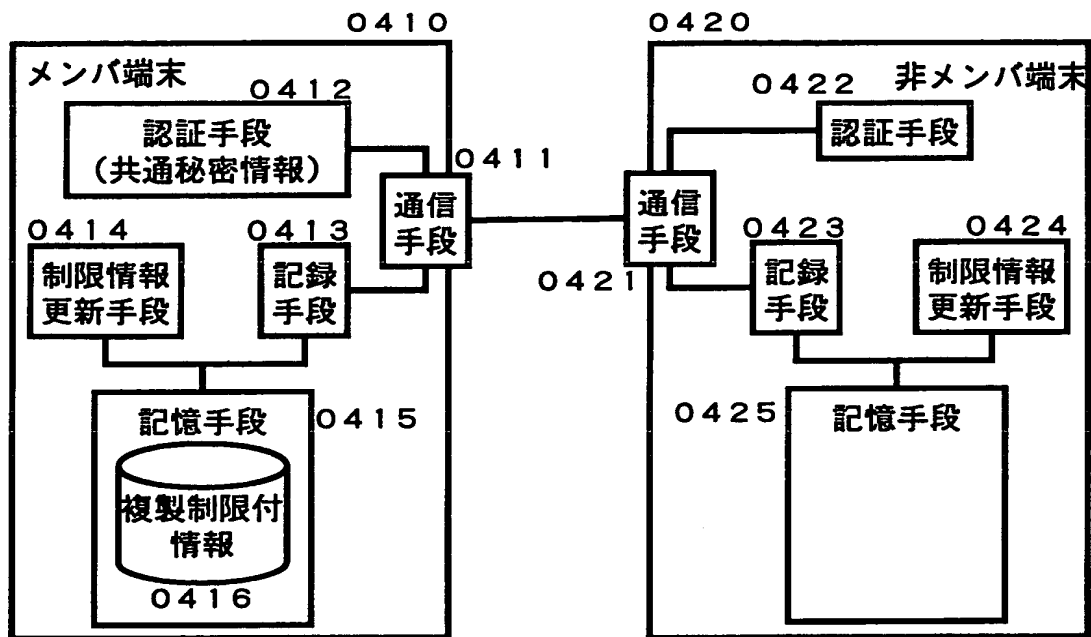
【図 2】



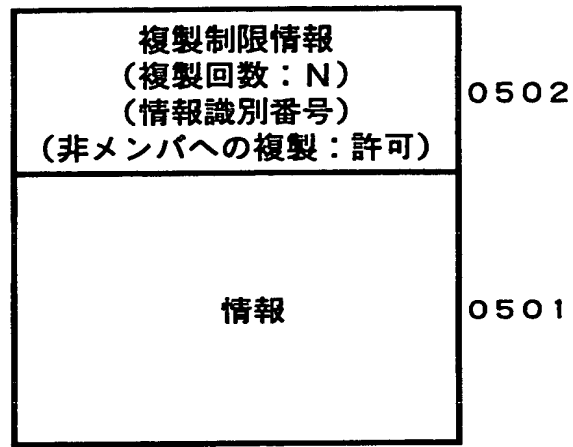
【図 3】



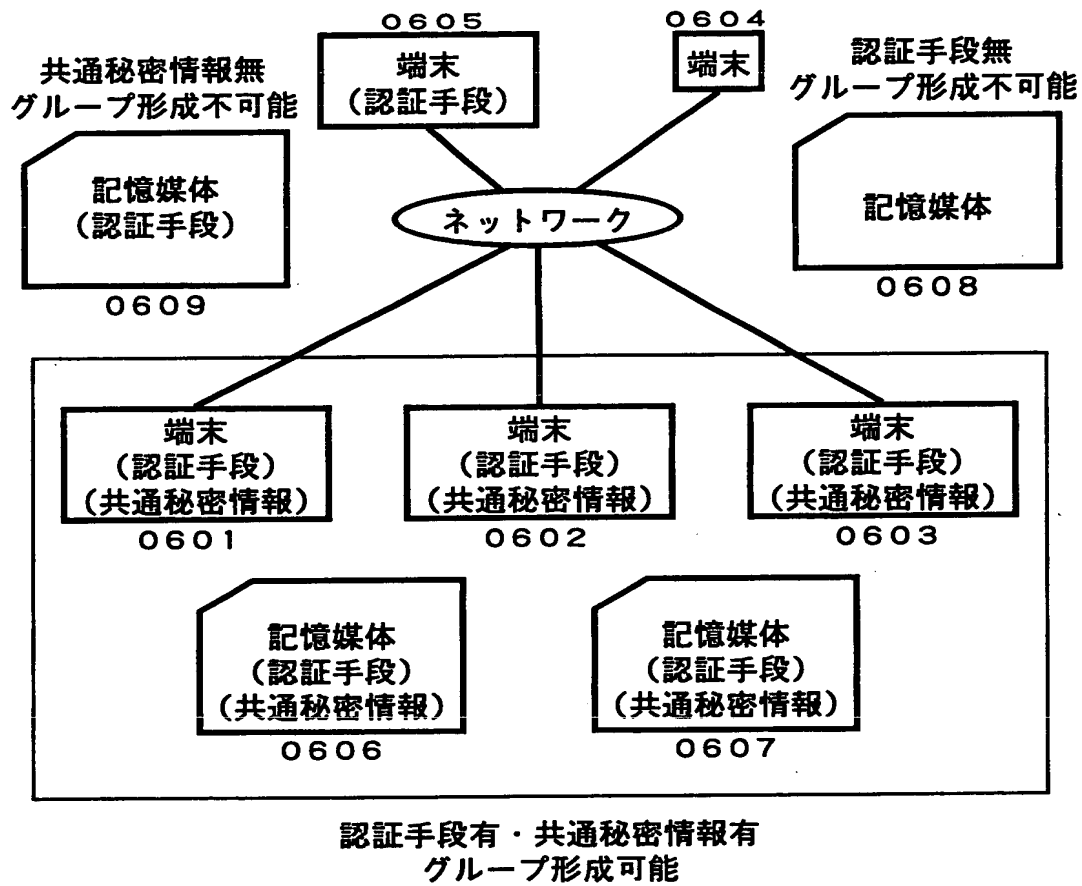
【図 4】



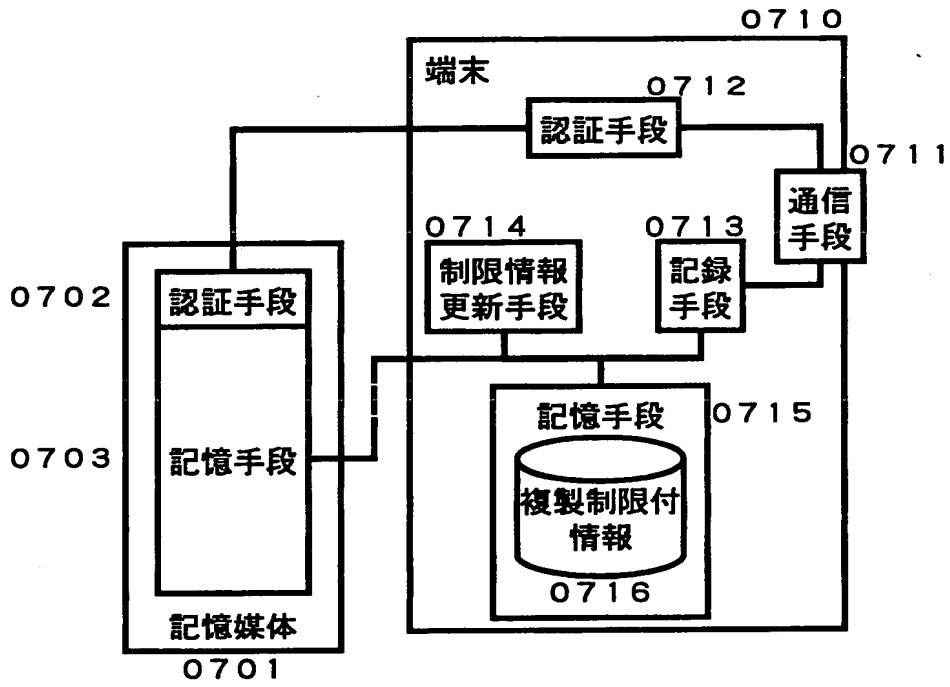
【図 5】



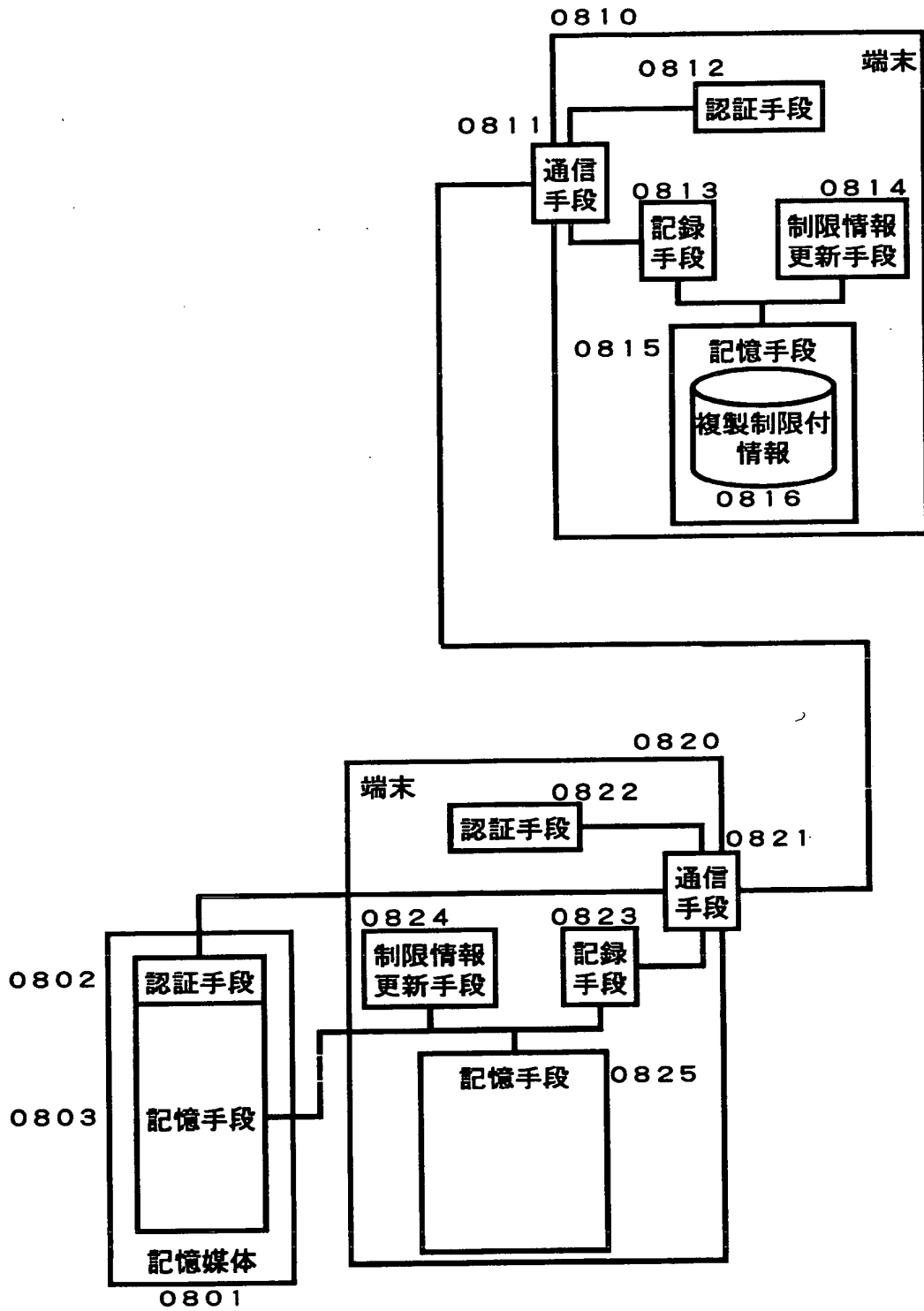
【図6】



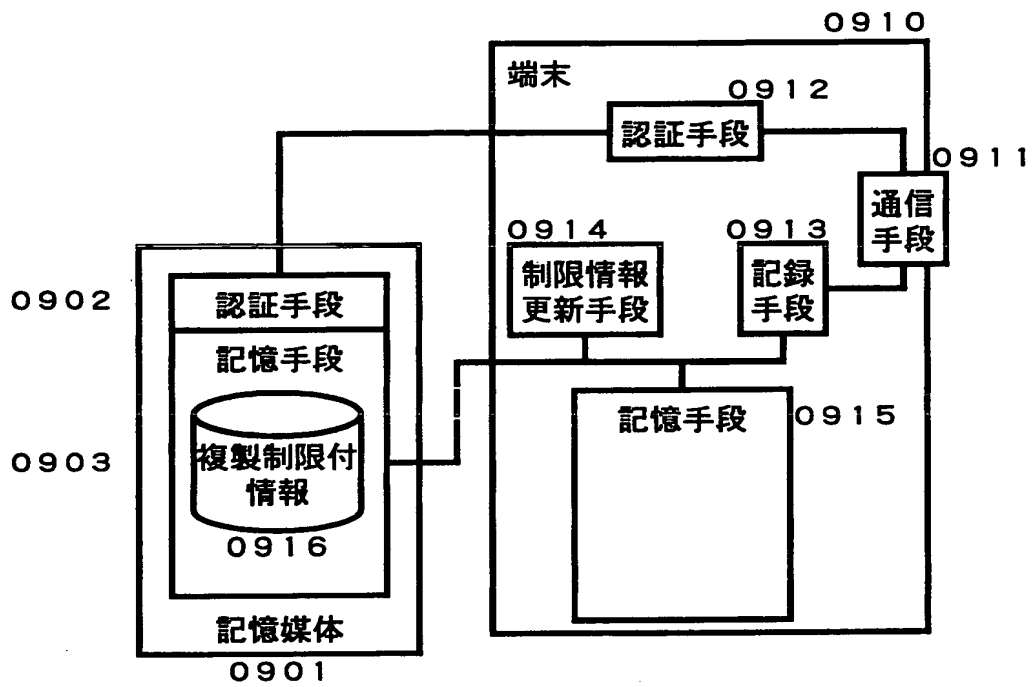
【図 7】



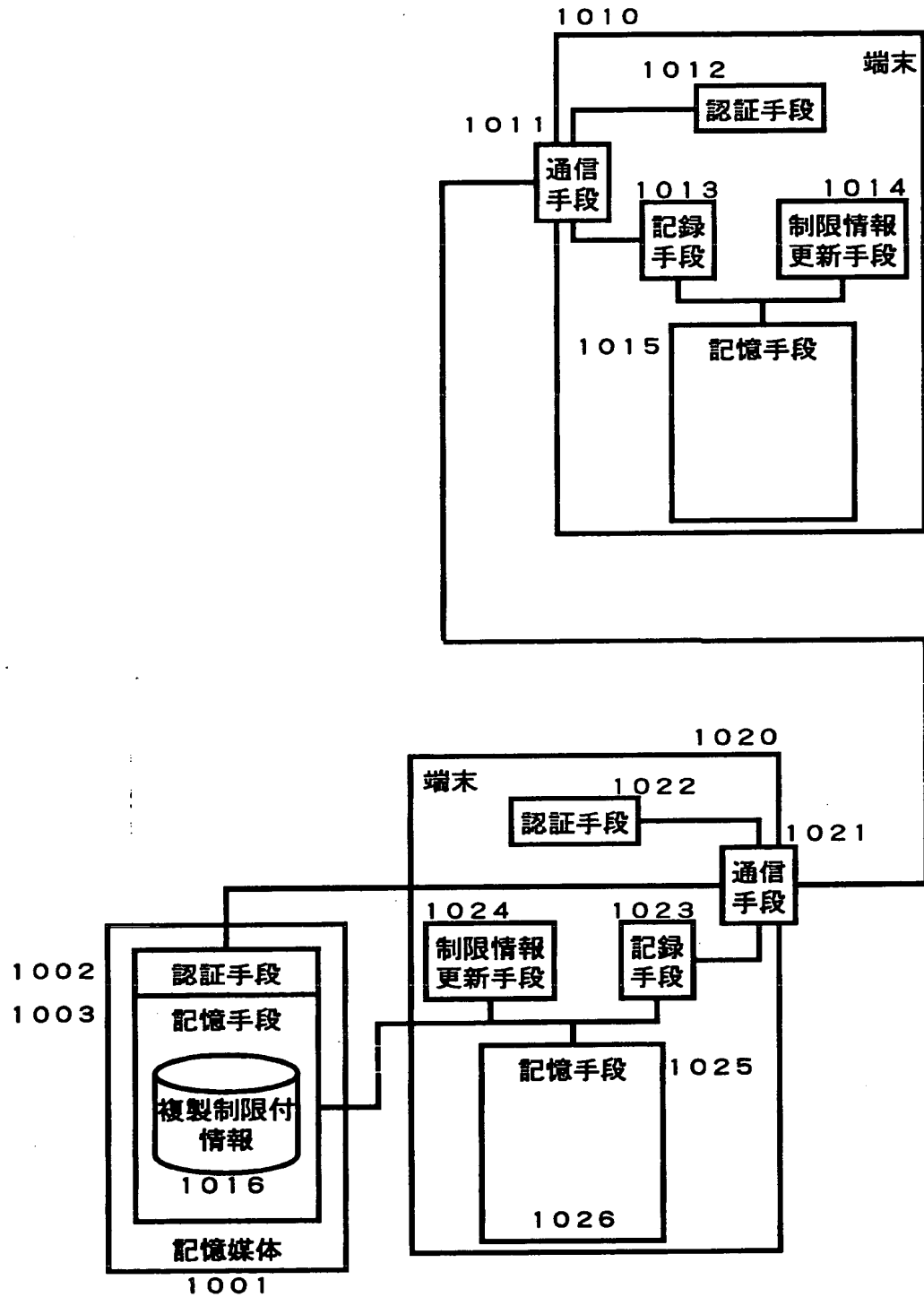
【図 8】



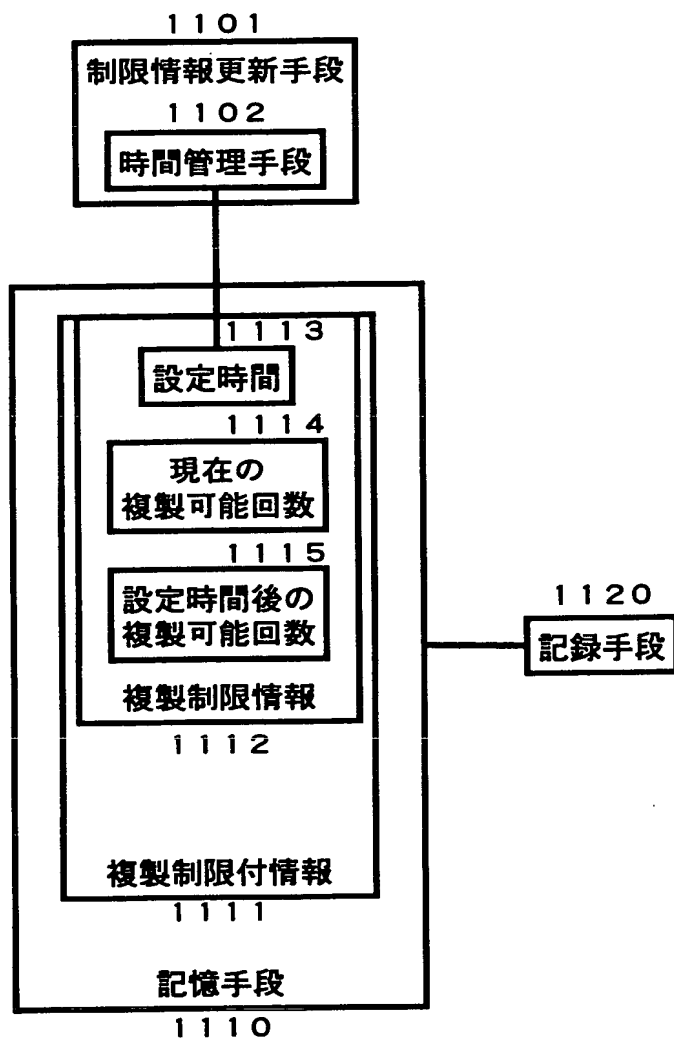
【図 9】



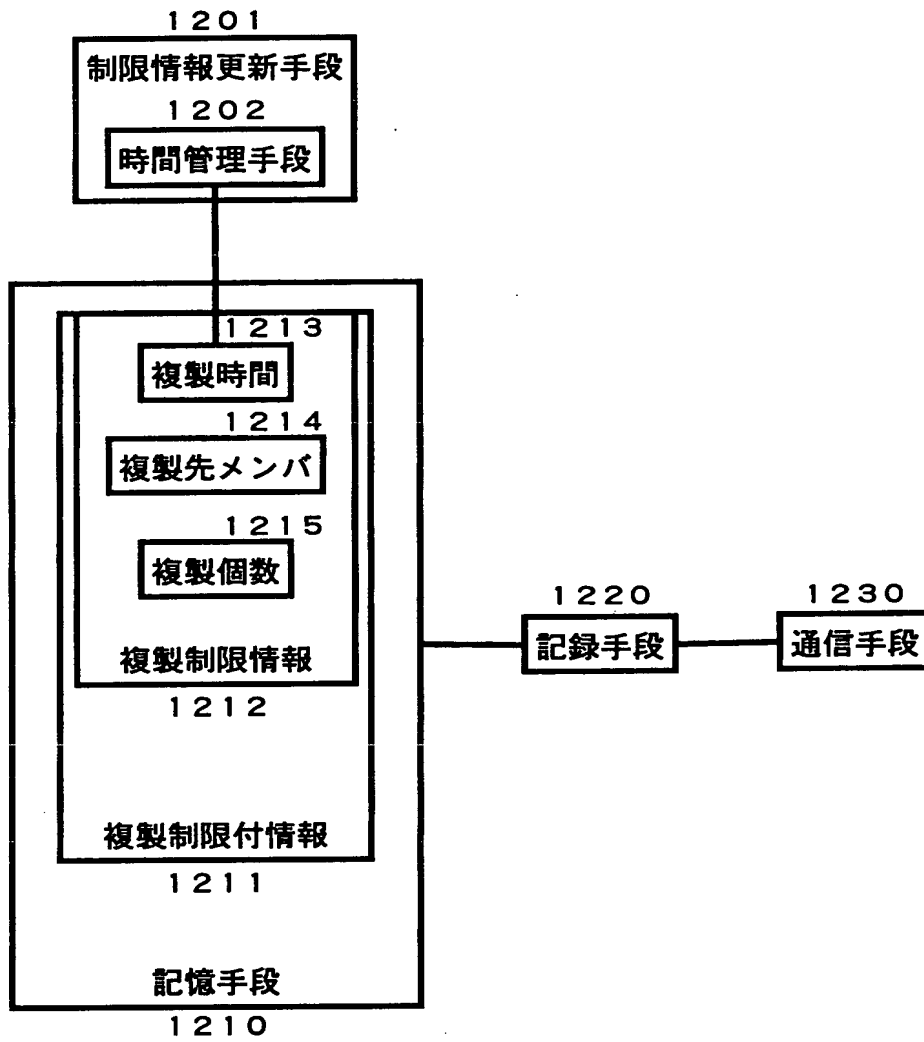
【図 1 0】



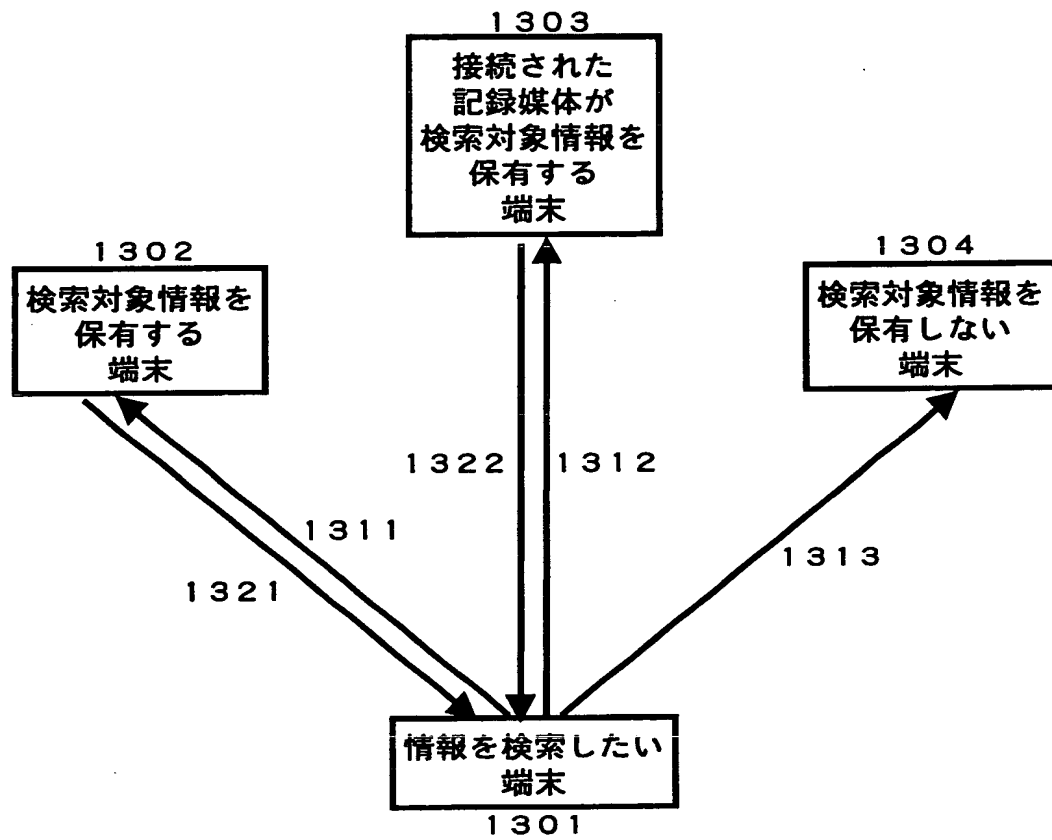
【図 1 1】



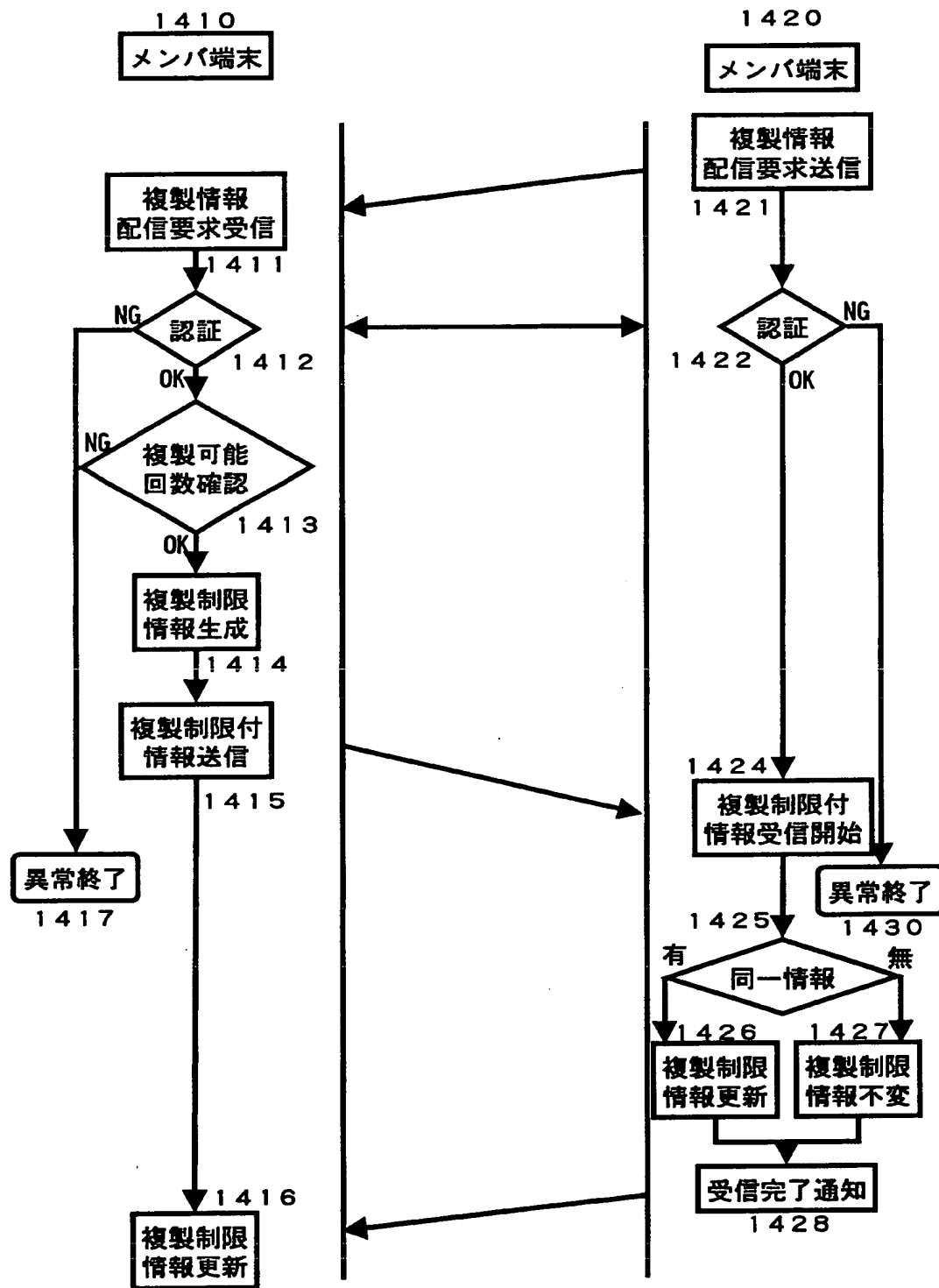
【図 1 2】



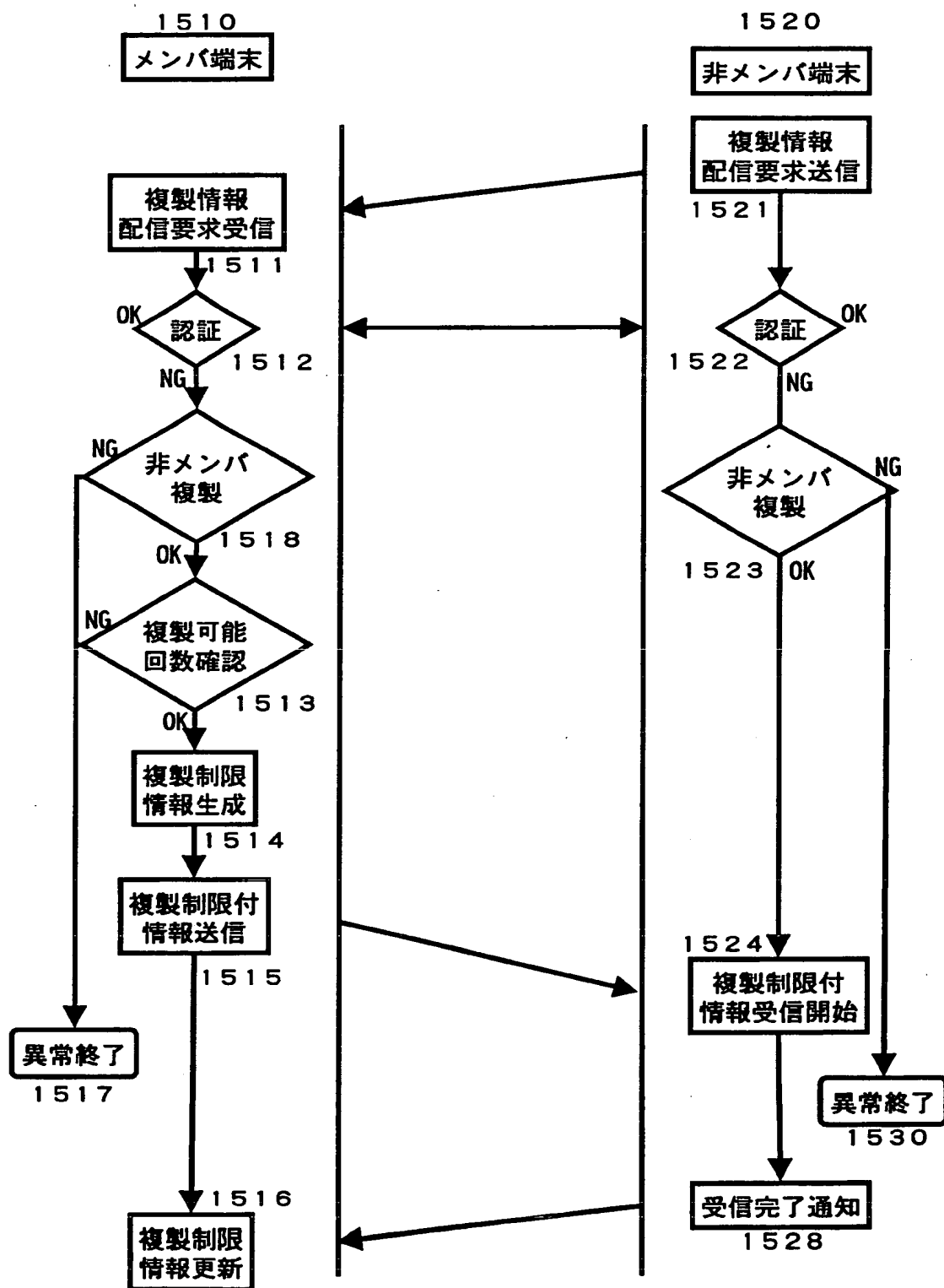
【図13】



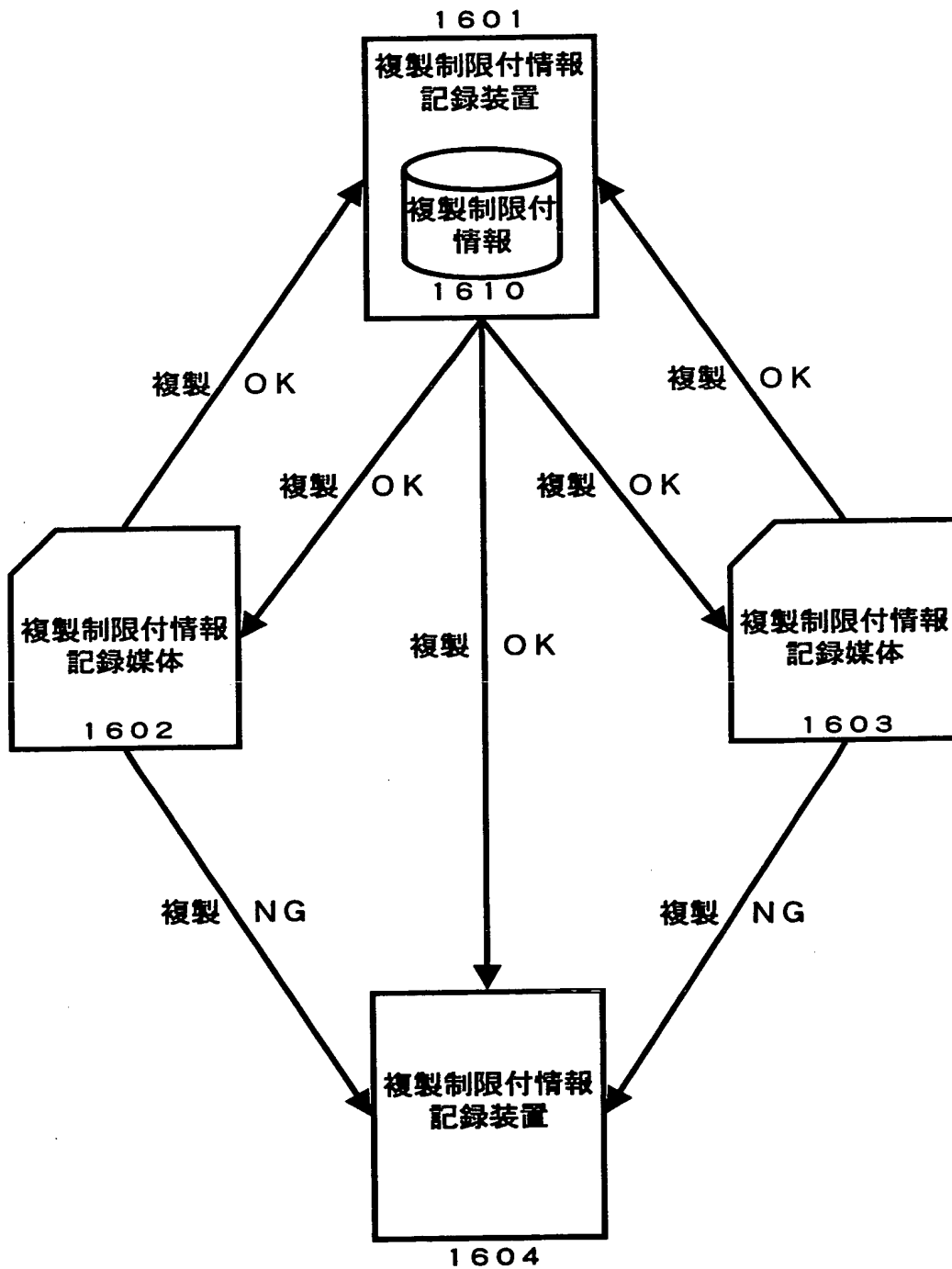
【図14】



【图 15】



【図16】



【書類名】 要約書

【要約】

【課題】 複製に関する制限が設けられた情報の複製について、複製する側とされる側との複製の制限に関する情報を更新することにより、自由度の高い情報複製管理ネットワークシステムおよび記録媒体を提供することを目的とする。

【解決手段】 複製する端末と複製される端末または記録媒体をネットワークで接続し、認証手段により複製される側の正当性を確認し、制限情報更新手段により、情報を複製する際に、複製する側とされる側との複製の制限に関する情報を更新し、通信手段を介して、複製する側の記録手段から複製される側の記憶手段へ複製する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日
[変更理由] 新規登録
住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社